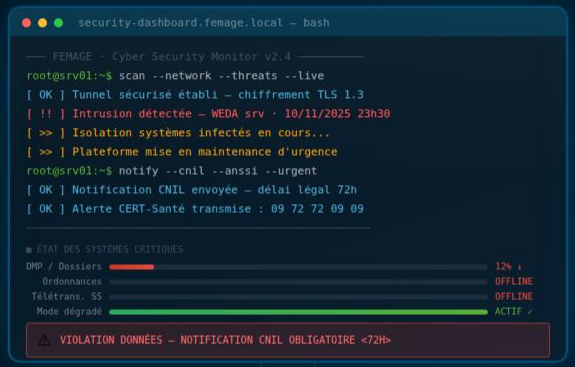

WEBINAIRE FORMATION — FEMAGE GRAND-EST

RGPD en santé : ce que vous devez savoir en 1 heure

Cyberattaques · Obligations légales · Mode dégradé · Responsabilité juridique · Plan de crise ACI

23 000	72 H	33 M	ART.32
SOIGNANTS PARALYSÉS WEDA — NOV. 2025	DÉLAI LÉGAL NOTIFICATION CNIL OBLIGATOIRE	DONNÉES DE SANTÉ COMPROMISES EN 2024	RGPD — OBLIGATION DE SÉCURITÉ

Cybersécurité · RGPD · Maisons de Santé · ACI 2025 · Mode dégradé · Plan de crise · WEDA · Cegedim

WEDA — 10 nov. 2025
Ransomware · 23 000 professionnels impactés

CEGEDIM — 2020/2024
Paralysie facturation & télétransmission SS

VIAMEDIS/ALMERYS — fév. 2024
33 millions d'assurés exposés

FEMAGE

WEBINAIRE
30 avril 2026

Objectifs du webinaire

Comprendre vos obligations réelles au regard du RGPD (Règlement Générale sur la Protection des données)

Identifier les points de vigilance propres aux MSP et CPTS : données patients, partage d'informations, logiciels métier…

Connaître vos responsabilités en tant que professionnel de santé ou coordinateur, notamment en cas de cyberattaque ou de fuite de données

Repartir avec des outils concrets : une check-list pratique directement applicable dans votre structure, modèle de registre des traitements, etc.

La mise en conformité

En MSP, la responsabilité est double

Obligations de la SISA	Obligations du professionnel à titre individuel
✓ Désigner un DPO (Délégué à la Protection des Données) ou référent RGPD ✓ Tenir le Registre des activités de traitement ✓ Rédiger ou actualiser les mentions d'information patients ✓ Conclure des contrats de sous-traitance avec les éditeurs logiciels ✓ Mettre en place une politique de sécurité des données ✓ Déclarer les violations de données à la CNIL (Commission Nationale de l'informatique et des libertés) sous 72 h ✓ Former le personnel aux bonnes pratiques	✓ Respecter le secret médical et la confidentialité ✓ Tenir le Registre des activités de traitement individuel ✓ Respecter la politique de sécurité des données de la structure ✓ Ne pas transmettre de données patients par email non sécurisé ✓ Signaler immédiatement tout incident ou doute à la SISA ✓ Participer aux formations internes RGPD

Certains traitements partagés (dossier patient, coordination des soins) font de la SISA et des professionnels des coresponsables : un accord écrit est alors obligatoire pour définir les rôles de chacun.

La mise en conformité

Le registre des traitements

C'est LE document central de votre conformité.
Il recense tous les traitements de données réalisés dans votre structure.
Il se présente sous forme de fiches
(un traitement de données = une fiche traitement)

Identification

- Intitulé du traitement
- Finalité
- N° de fiche dans le registre

Responsabilité

- Responsable de traitement (SISA)
- Coresponsables + accord
- Coordonnées DPO / référent RGPD

Base légale

- Base légale (consentement, intérêt public...)
- Articles RGPD applicables

Personnes & données

- Catégories de personnes concernées
- Catégories de données traitées
- Données sensibles (art. 9) ?

Accès & circulation

- Destinataires internes
- Destinataires externes / sous-traitants
- Transfert hors UE + garanties

Conservation

- Durée de conservation
- Modalités d'archivage / suppression

Sécurité & outils

- Logiciels / outils utilisés
- Hébergeur + certification HDS
- Mesures de sécurité (techniques & orga.)

Analyse de risque

- PIA nécessaire ? (oui / non / à évaluer)
- Référence au document PIA si applicable

Suivi

- Date de création
- Date de mise à jour
- Nom du référent

Un registre des traitements prérempli pour les MSP est disponible dans la boîte à outils FEMAGE

La mise en conformité

Informer vos patients de l'utilisation de leurs données

L'obligation d'information

Chaque patient doit être informé :

- De la finalité du traitement de ses données
- De l'identité du responsable de traitement
- Des destinataires (autres professionnels, SI…)
- De la durée de conservation
- De ses droits : accès, rectification, effacement, opposition, portabilité

Cette obligation s'appelle le droit à l'information

Comment vous conformer ?

✅ Afficher une note d'information dans la salle d'attente

✅ Intégrer une mention dans vos formulaires de recueil de consentement, site web… etc.

✅ Informer oralement lors du premier contact si nécessaire

✅ Mettre à jour les mentions lors de changements de logiciels ou de prestataires

📥 **Une affiche type est disponible dans la boîte à outils FEMAGE**

CABINET HOUDART ET ASSOCIÉS

Droit Numérique

Santé Numérique

RGPD

Raphaël CAVAN

Avocat spécialisé en droit Numérique

Pôle Santé Numérique

Droit du numérique en santé

Conseil et contentieux RGPD, hébergement de données de santé (HDS), sécurité des systèmes d'information.

Structures de santé

Accompagnement des MSP, CPTS, centres de santé dans leur mise en conformité et gestion des incidents.

Gestion des risques juridiques

Analyse des responsabilités, contrats DPA, procédures CNIL, réponse aux violations de données.

Les schémas de responsabilité RGPD

1ER SCHÉMA — Responsable de Traitement distinct

La structure d'exercice coordonné (MSP / SISA) et les associés sont chacun Responsable de Traitement (RT) de leurs outils respectifs — aucune co-responsabilité n'est établie.

MSP / SISA
Responsable de Traitement du SIP

Obligations SISA

- ✓ Désigner un DPO ou référent RGPD
- ✓ Registre des traitements (Art. 30)
- ✓ Analyse d'impact (AIPD) si requis
- ✓ Contrats DPA avec les éditeurs

Pas de co-responsabilité

Professionnels de santé
Responsables de Traitement de leurs outils

Obligations individuelles

- ✓ Registre des traitements individuel
- ✓ Analyse d'impact (AIPD) sur leurs outils
- ✓ Respect de la politique de sécurité
- ✓ Signaler tout incident à la SISA

Les schémas de responsabilité RGPD

2ÈME SCHÉMA — Co-Responsables de Traitement (Co-RT)

La structure d'exercice coordonné et les associés sont Co-Responsables de Traitement (Co-RT) du SIP. Un accord écrit de Co-RT est alors obligatoire pour définir les rôles de chacun.

ACCORD DE CO-RESPONSABILITÉ (obligatoire)

MSP / SISA
Co-Responsable de Traitement du SIP

Professionnels de santé
Co-Responsables de Traitement du SIP

Obligations SISA (Co-RT)

- ✓ DPO + Registre des traitements + AIPD sur le SIP
- ✓ Définir les rôles dans l'accord de Co-RT
- ✓ Point de contact commun pour les patients

Obligations individuelles (Co-RT)

- ✓ Registre des traitements + AIPD sur leurs outils propres
- ✓ RT de leurs logiciels individuels
- ✓ Respecter les termes de l'accord de Co-RT

Le rôle du DPO

Délégué à la Protection des Données

Le DPO (ou référent RGPD pour les MSP non soumises à l'obligation) est le pivot de la conformité. Il n'est pas responsable des manquements mais pilote et conseille.

⚙️ Pilote la conformité

Coordonne la mise en œuvre de la politique RGPD au sein de la structure et tient le registre des traitements à jour.

🔔 Point de contact CNIL

Interlocuteur privilégié de l'autorité de contrôle (CNIL). Assure les notifications en cas de violation de données.

DPO

Référent RGPD

(Facultatif pour les MSP non soumises à l'obligation)

🎓 Conseil et accompagnement

Conseille la structure, les professionnels et les sous-traitants. Anime la formation RGPD de l'équipe.

📋 Gestion des droits

Traite les demandes d'exercice des droits des patients (accès, rectification, effacement, opposition).

La violation de données

Qu’est ce qu’une violation de données ?

3 FORMES DE VIOLATION

Confidentialité
Données vues par une personne non autorisée

Disponibilité
Données inaccessibles ou perdues

Intégrité
Données modifiées ou corrompues

Aussi une violation :
Perte/vol d’un appareil (ordinateur, clé USB…)
Envoi au mauvais destinataire
Accès non autorisé à un dossier
Destruction ou altération de données

LES 3 CYBERMENACES PRINCIPALES

Ransomware — Disponibilité

Logiciel malveillant qui **bloque l’accès aux fichiers** et réclame une rançon. Peut paralyser la structure pendant plusieurs jours.

Phishing — Porte d’entrée

Email imitant un organisme de confiance (CPAM, éditeur…) pour **voler des identifiants**. Souvent le point de départ d’une attaque plus large.

Intrusion — Confidentialité

Accès non autorisé au système par exploitation d’une faille. Peut rester **silencieux plusieurs semaines** avant d’être détecté.

⚠ Toute violation doit être **consignée dans le registre des violations** — même si elle ne nécessite pas de notification à la CNIL

La violation de données

Vos obligations RGPD immédiates

- ➔ Stopper l'accès non autorisé, isoler les systèmes compromis, alerter le référent RGPD ou le DPO
- ➔ Evaluer le risque pour les personnes concernées
- ➔ Consigner l'incident dans votre registre des violations et les mesures correctives
- ➔ Se référer à la fiche réflexe de l'ARS (cf boîte à outil FEMAGE)

72 h

Notification CNIL

Signaler toute violation de données personnelles dans les 72h suivant la découverte

Sans délai

Notification patients

Si risque élevé pour les droits des personnes, informer les patients concernés sans délai

5 ans

Registre des violations

Documenter et conserver la trace de tout incident de sécurité dans le registre interne des violations

Avant tout

Mesures techniques

Démontrer que des mesures de sécurité appropriées étaient en place avant l'incident

Mode dégradé

Organisation concrète du cabinet en cas de panne ou cyberattaque

🗂️ Gestion Patients

- Registre papier des consultations du jour
- Ordonnances manuscrites (tampon + signature)
- Carnet de vaccination accessible hors SI
- Coordonnées d'urgence affichées
- Accès aux résultats via messagerie sécurisée (si disponible)

👥 Gestion Équipe

- Informer immédiatement tout le personnel
- Désigner un référent de crise
- Liste de contacts clés imprimée (éditeur SI, RSSI, CPAM…)
- Activer les protocoles de communication dégradée
- Soutien psychologique si nécessaire

💼 Administratif

- Feuilles de soins papier (FSP) pour la facturation
- Registre des actes papier
- Conserver tous les documents produits
- Documenter la durée de l'interruption
- Contacter le support CPAM si besoin

💡 **Préparez un classeur mode dégradé accessible sans ordinateur : formulaires vierges, annuaires, protocoles imprimés**

Cybersécurité — Risques juridiques

RISQUES JURIDIQUES — Ce que vous risquez concrètement

Responsabilité administrative (RGPD)

CNIL — Sanctions

Manquement Art. 32 : obligation de sécurité des données

Sanctions simplifiées récentes :

→ Médecin généraliste : 3 000 € (2025)

→ Chirurgien-dentiste : 4 000–5 000 € (2024)

→ Médecin généraliste : 4 000 € (2024)

→ Orthophoniste : 4 000 € (2024)

→ Clinique : 15 000 € (2024)

Responsabilité civile

Préjudice moral

Fondement : Art. 1240 Code civil + Art. 82 RGPD

CJUE, 4 mai 2023, C-300/21 :

Encadre la reconnaissance d'un préjudice moral lié au RGPD

TA Montpellier, 20 juin 2025 :

1 500 € de dommages et intérêts pour divulgation de données personnelles

Responsabilité pénale

Secret médical

Violation du secret médical :

Art. 226-13 du Code pénal

Sanctions encourues :

→ 1 an d'emprisonnement

→ 15 000 € d'amende

En cas de mise en danger délibérée des patients

⚠ **Toute violation doit être consignée dans le registre des violations — même si elle ne nécessite pas de notification à la CNIL**

Anticiper

Les mesures préventives

💾 Sauvegardes régulières

Sauvegarde quotidienne, hors ligne, testée régulièrement. Règle 3-2-1 : 3 copies, 2 supports, 1 hors site.

🔑 Gestion des accès

Mots de passe robustes, MFA activé (authentification multi facteur), comptes nominatifs. Droits d'accès limités au strict nécessaire.

🔒 Chiffrement des données

Chiffrement des postes et des sauvegardes. Messagerie chiffrée (MSSanté) pour les données de santé.

🛡️ Protection du réseau

Pare-feu actif, Wi-Fi patients séparé du réseau professionnel, VPN pour les accès distants.

📋 Plan de crise écrit

Document formalisé : contacts, procédures, mode dégradé. Intégrable dans le plan de situation sanitaire exceptionnelle du projet de santé / ACI.

🎓 Information de l'équipe

Sensibilisation au phishing, gestion des mots de passe, signalement des incidents suspects. Diffusion de la charte informatique.

Plan d'action

Ce que vous devez faire dès demain

A faire en priorité	Mise en place du registre des traitements et de la charte informatique
A faire en priorité	Imprimer et plastifier la fiche réflexe à chaque poste
A faire en priorité	Vérifier que les sauvegardes fonctionnent et sont déconnectées du réseau
Dans la foulée	Rédiger / mettre à jour le plan de crise cyber de votre structure (modèle ACI)
Quand vous pouvez	Former l'équipe à la détection du phishing et aux bons réflexes
Quand vous pouvez	Souscrire une assurance cyber professionnelle adaptée
Pour aller plus loin	Tester le plan de crise et engager une réflexion collective sur le DPO

La cybersécurité n'est pas une question de "si" mais de "quand" — Anticipez !

✅ Ce qu'il faut retenir

1 📋 Tenez votre registre

Le registre des traitements (Art. 30) est obligatoire. La FEMAGE vous fournit un modèle pré-rempli.

2 👥 Informez vos patients

Chaque patient doit être informé de l'utilisation de ses données (Art. 13). Affichez la note d'information.

3 🔒 Sécurisez vos systèmes

Sauvegardes hors ligne, mots de passe robustes, MFA : des mesures simples qui peuvent tout changer.

4 ⏱️ 72h pour notifier la CNIL

En cas de cyberattaque avec violation de données, vous avez 72h pour déclarer l'incident à la CNIL.

5 📄 Préparez votre fiche réflexe

Un plan de crise imprimé et affiché sauve du temps précieux. Téléchargez le modèle FEMAGE.

6 🎓 Formez votre équipe

La majorité des cyberattaques commencent par un phishing. La sensibilisation est votre meilleur bouclier.

Boîte à outils RGPD

Tous les documents disponibles sur le site FEMAGE

📥 Tout télécharger

Conformité

Check-list RGPD

Liste de contrôle pratique MSP

Communication

Affiche RGPD

Information patients salle d'attente

Conformité

Registre des traitements

Art. 30 RGPD pré-rempli MSP

Sécurité

Registre des violations

Traçabilité obligatoire des incidents

Sécurité

Charte informatique

À faire signer par chaque utilisateur

Crise

Fiche réflexe

Protocole urgence cyberattaque 72h

Avancé

PIA / AIPD

Analyse d'impact protection des données

Juridique

DPA / Contrat sous-traitant

Art. 28 RGPD avec les éditeurs

FEMAGE
Grand-Est

Merci pour votre participation !

Webinaire RGPD en santé — FEMAGE Grand-Est · 30 avril 2026

🙏 Remerciements au Cabinet Houdart et Associés

Raphaël CAVAN
Avocat spécialisé en droit Numérique — Pôle Santé Numérique

👥 Merci à tous les participants

Professionnels de santé, coordinateurs et équipes des MSP et CPTS Grand-Est — votre engagement pour la conformité RGPD protège vos patients et vos structures.

⭐ Questionnaire de satisfaction

Votre retour nous aide à améliorer nos webinaires — merci !

📊 Questionnaire satisfaction

🧰 Boîte à outils FEMAGE

www.femage.fr/ressources-rgpd

Téléchargez tous les modèles et outils